Raymond P. Boucher, State Bar No. 115364
ray@boucher.la
Shehnaz M. Bhujwala, State Bar No. 223484
bhujwala@boucher.la
BOUCHER LLP
21600 Oxnard Street, Suite 600
Woodland Hills, California 91367-4903
Tel: (818) 340-5400; Fax: (818) 340-5401

Raina C. Borrelli (*Pro Hac Vice)*
raina@straussborrelli.com
Carly M. Roman (State Bar No. 3479895)
croman@straussborrelli.com
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: (872) 263-1100; Fax: (872) 263-1109

Interim Co-Lead Class Counsel

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

IN RE JAIME S. SCHWARTZ, MD, DATA SECURITY LITIGATION

Lead Case: 2:25-CV-00898-GW-SSC

Consolidated Cases:
2:25-cv-02263
2:25-cv-03993
3:25-cv-00576

CLASS ACTION

CONSOLIDATED COMPLAINT FOR DAMAGES, DECLARATORY, AND INJUNCTIVE RELIEF FOR:

1. **VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMATION ACT;**
2. **NEGLIGENCE;**
3. **VIOLATION OF THE UNFAIR COMPETITION LAW [Cal. Bus. & Prof. Code § 17200];**
4. **INVASION OF PRIVACY;**
5. **VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, *et seq.*;**

6. BREACH OF IMPLIED CONTRACT;

7. UNJUST ENRICHMENT; AND

8. VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT, CIVIL CODE § 1798.150, *et seq*

DEMAND FOR JURY TRIAL

Plaintiffs JANE DOE A, an individual, JANE DOE B, an individual, JANE DOE C, an individual, JANE DOE D, an individual, and JANE DOE E, an individual (collectively, "Class Plaintiffs" or "Plaintiffs"),[1] on behalf of themselves and all others similarly situated ("Class Members"), allege for their complaint against Defendants JAIME S. SCHWARTZ, MD, a California professional corporation, JAIME S. SCHWARTZ, MD PC, a California professional corporation (collectively, "Dr. Schwartz"); TOTAL LIPEDEMA CARE, a California corporation (collectively, "Schwartz Defendants"); MEDVA, LLC, a Nevada corporation ("MEDVA"); MODERNIZING MEDICINE, INC., a Delaware Corporation ("ModMed"); and DOES 1 through 10, inclusive (collectively with Dr. Schwartz, "Defendants") as follows. Allegations herein are made on personal knowledge as to Class Plaintiffs and information and belief as to all other matters.

INTRODUCTION

1. Dr. Schwartz is a prominent plastic surgeon with offices in Beverly Hills and Dubai, including Total Lipedema Care in Beverly Hills, California. He has appeared on television networks Bravo and E! and was a featured doctor on the hit shows "Botched" and "The Doctors." Dr. Schwartz boasts total annual revenue of between $10 million and $25 million.

[1] Plaintiffs are identified in this Consolidated Complaint by letter as Jane Does A through E to avoid confusion with the designations in the separate complaints previously filed in the consolidated actions.

2. On his website, Dr. Schwartz proclaims that he "respect[s]" and is "committed to protecting" patient privacy. He promises patients: "As our patient, we want you to know that we respect the privacy of your personal medical information and will do all we can to secure and protect your privacy. We strive to always take reasonable precautions to protect your privacy."

3. MEDVA provides virtual assistants to medical practices. On information and belief, the Schwartz Defendants contracted with MEDVA to provide virtual administrative assistance and its employees or agents maintained access to the Schwartz Defendants' electronic records systems, including but not limited to medical files of patients.

4. ModMed provides specialty-specific health information technology solutions, including cloud-based electronic health records (EHR) systems, practice management, revenue cycle management, and telehealth services. On information and belief, the Schwartz Defendants contracted with ModMed to provide health information technology solutions used by Defendants that managed, maintained, and/or stored patients confidential medical information, including those systems which were compromised as alleged below. ModMed contracted to provide technology and related services, including EHR systems, to manage patients' sensitive medical data.

5. Despite charging clients thousands of dollars and having access to their deeply private medical information, Schwartz Defendants, MEDVA, and ModMed disregarded basic security measures necessary to protect that information from malicious cyberattacks. Dr. Schwartz and others in the medical field – and in the plastic surgery field specifically – have been warned for years by government agencies and professional organizations that they are targets for hackers who seek sensitive patient data for ransom and extortion.

6. ModMed also failed to provide minimally adequate computer systems and data security practices, necessary to protect sensitive medical information.

7. Schwartz Defendants, MEDVA, and ModMed disregarded frequent warnings and failed to take patient data security seriously. As a result of this negligence, Defendants allowed their network to be compromised ***twice*** in less than a year. On information and belief, the malicious actors gained access to Schwartz Defendants' entire network and all or substantially all patient data, including, most egregiously, nude and/or partially nude photos and videos of patients obtained during the course of consultation and treatment combined with personal information.

8. On information and belief, the hackers stole private personal and medical data from thousands of patients to use in an effort to extort Dr. Schwartz and the patients. This included 1.1 terabytes of patient data, reflecting almost 250,000 unique files. The private data included, among other things, nude and/or partially photographs and video of patients with both their faces and private parts visible, as well as images taken during surgery reflecting patients' ongoing surgical procedures.

9. Not only did Schwartz Defendants fail to notify his patients or law enforcement as required, but he actively hid the first hack. Defendants failed to take reasonable measures to secure their network, even after learning of the first hack.

10. Approximately six months later, in March of 2024, Schwartz Defendants' system was hacked again by a different hacker group. On information and belief, the second hacker group also gained access to the entire system and all or substantially all patient data. On information and belief, they successfully exfiltrated (*i.e.*, downloaded) over 1,700 patient files.

11. Once again, however, Dr. Schwartz attempted to sweep the second hack under the rug. He failed to notify his patients as required by federal and state law. Instead, he waited to do so until after the hackers posted a ***public website*** (the "Hacker Website"), announcing the hack and leaking names, contact information, and nude photographs, and began attempting to directly extort patients to remove their data. Despite knowing that his patients' most private medical data was in the hands of malicious actors, Dr. Schwartz waited almost 10 months to notify them.

12. To date, the hackers have posted approximately 80 patient files, complete with names, dates of birth, phone numbers, home addresses, and nude photos – including photos of unconscious patients during surgery.[2] They have warned that they will continue releasing patient files until Dr. Schwartz's contacts them.

13. In addition to the usual array of plastic surgery offerings, such as liposuction and breast augmentation, Dr. Schwartz specializes in treatment of lipedema which involves the abnormal buildup of fat in the lower body, specifically the buttocks, thighs, and calves, as well as other areas.

14. Lipedema is a painful and potentially disfiguring chronic medical condition frequently associated with a range of comorbidities, including obesity, anxiety, depression, and eating disorders. These comorbidities are often exacerbated by the psychological impact of the disease and by the mistreatment many lipedema patients experience within the medical system. Such mistreatment commonly includes fat-shaming, patient-blaming, and a refusal by healthcare providers to acknowledge or validate patients' self-reported symptoms and medical histories.

15. As a result, women with lipedema often experience profound body-related anxiety and shame, particularly regarding the affected areas of their bodies. This leads to extreme emotional distress when their bodies, especially the lipedema-affected regions, are exposed or seen by others.

16. Class Plaintiffs are patients of Schwartz Defendants and victims of the cyberattacks. They sought medically necessary treatment from Dr. Schwartz to address their lipedema on the understanding that their treatment and medical records would be kept strictly confidential. As a result of this treatment, Dr. Schwartz and his staff obtained extensive medical information about Class Plaintiffs and other patients, including the types of information, photographs, and videos outlined above. With respect to Class Plaintiffs and many others, these photographs and videos include detailed, nude and semi-nude images of their pelvic areas, breasts, thighs, and

[2] During the pendency of this action, the hackers have posted another 30 patient files.

buttocks, including images and video taken during surgery.

17. On information and belief, all this information was exfiltrated from Schwartz Defendants' network / EHR system during the recent cyberattack. All Class Plaintiffs have been threatened with the imminent release of this deeply private information. Certain Class Plaintiffs have already had their data, including photographs, leaked online. It is only a matter of time before the hackers release the names, home addresses, medical information, and private images of Dr. Schwartz's other patients.

18. Plaintiffs bring this action for injunctive relief to rectify Dr. Schwartz's negligent cybersecurity practices and to require him to destroy or secure any private personal and medical information in his possession. They also seek statutory damages and damages for the severe emotional toll that having their private medical information compromised has taken on them.

PARTIES

Class Plaintiffs

19. Plaintiff Jane Doe A is an individual and citizen of the State of California.

20. Plaintiff Jane Doe B is an individual and citizen of the State of Michigan.

21. Plaintiff Jane Doe C is an individual and citizen of the State of Arkansas.

22. Plaintiff Jane Doe D is an individual and citizen of the State of Oregon.

23. Plaintiff Jane Doe E is an individual and citizen of the State of California.

24. Plaintiffs sue under these pseudonyms pursuant to *Does I through XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1067 (9th Cir. 2000) and the Court's October 6, 2025 order granting permission to proceed under these pseudonyms.

Defendants

25. Defendant Jaime S. Schwartz, MD is an individual and, on information and belief, a resident of Los Angeles County, California. Dr. Schwartz owns and operates Jaime S. Schwartz, MD PC.

26. Defendant Jaime M. Schwartz, MD PC is a California professional corporation with its principal place of business in Beverly Hills, California. Jaime S. Schwartz, MD PC operates two plastic surgery practices in Beverly Hills and Dubai.

27. Defendant Total Lipedema Care is a California corporation with its principal place of business in Beverly Hills, California. On information and belief, Total Lipedema Care is owned and controlled by Dr. Schwartz, and was used as a vehicle to market medical services to and provide treatment to patients suffering Lipedema. Total Lipedema Care's operations are headquartered in Beverly Hills, California, at the offices of Dr. Schwartz, where they oversee all corporate policies, including data security.

28. MEDVA is a Nevada Corporation with its principal address in Henderson, Nevada. On information and belief, MEDVA conducts significant business in California, including within Los Angeles County. According to filings with the California Secretary of State, MEDVA maintains a California office located at 440 N. Barranca Ave #1122, Covina, California 91723 and its two founding members, Dr. Omid Shaye and Dr. Steven Kupferman, list that California address in filings as their addresses. On information and belief, both members appear to practice medicine and reside in Los Angeles, California.

29. ModMed is a Delaware Corporation with its principal place of business in Boca Raton, Florida. On information and belief, ModMed conducts significant business in California, including with Dr. Schwartz.

30. Class Plaintiffs are currently unaware of the true names and capacities of Defendants Does 1 through 10 ("Doe Defendants"), inclusive, and so name them under these fictitious names. Class Plaintiffs are informed and believe that the Doe Defendants are in some manner legally responsible for the acts, omissions, and damages alleged herein. On information and belief, the Doe Defendants include the individuals and entities who were in part responsible for maintaining the security of Dr. Schwartz's computer system and network, and the individuals and entities

responsible for allowing the hack to take place. On information and belief, the Doe Defendants are principals, agents, partners, joint venturers, and alter egos of the other Defendants, acted in concert with the other defendants, aided and abetted the other Defendants, and conspired with the other Defendants in connection with the conduct alleged herein. Class Plaintiffs will seek leave to amend this Complaint to identify the true names and capacities of the Doe Defendants when the same become known.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332. The amount in controversy in this action exceeds $5,000,000, exclusive of interests and costs. There are more than 100 members in the proposed class. Plaintiffs estimate that the data breaches affected hundreds, if not thousands, of Dr. Schwartz's patients. At least one member of the class is a citizen of a state different from Defendants, as set forth above.

32. The Court has personal jurisdiction over Defendants who maintain their residence and principal place of business in this District, and who regularly transact business within the State of California.

33. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a majority of the Defendants reside in this District and a substantial part of the events, acts, and omissions giving rise to Class Plaintiffs' claims occurred in and emanated from this District, namely from the Schwartz Defendants' primary office in Beverly Hills, California.

34. California has a significant interest in regulating businesses operating within its jurisdiction, including the protection of consumers' rights and personal data.

35. Schwartz Defendants' operations are headquartered in Beverly Hills, California, from where they oversee all corporate policies, including data security for their medical practice and Total Lipedema Care, from within the state. Based on available information, decisions regarding Defendants' network security and response to the data breach originated from California.

36. Because Defendants' actions and failures to act occurred in California, California's laws are appropriately applied. Under California's choice of law principles, California law governs the nationwide claims of Plaintiffs and the Class.

37. Additionally, California's Unfair Competition Law, CMIA, and Consumer Privacy Act apply to non-resident Plaintiffs due to Defendants' business operations in California and the fact that the acts and omissions from which liability arose occurred in California.

ALLEGATIONS COMMON TO ALL CLAIMS

Dr. Schwartz's Medical Practice

38. Dr. Schwartz owns and operates a plastic surgery practice in Beverly Hills, California. He is a board-certified plastic surgeon and a member of the American Society of Plastic Surgeons ("ASPS"). According to his marketing materials, he is "an internationally recognized expert in plastic surgery, specializing advanced surgical techniques" and "nationally renowned" for plastic surgery.

39. Dr. Schwartz offers a wide array of services, primarily catering to women. Among other things, he is widely known for his accomplishments in the field of breast augmentation and reconstruction, offering a host of related services to patients. He also offers a series of other surgical options focusing on private areas of the body, such as liposuction, butt lifts and implants, cellulite reduction, and vaginal rejuvenation.

40. In addition to a wide array of cosmetic surgeries, Dr. Schwartz also specializes in medically necessary treatment for lipedema. Lipedema treatment involves highly invasive surgery to remove excess fat tissue from the buttocks, thighs, calves, and other areas, while preserving delicate lymph nodes and blood vessels.

41. Dr. Schwartz formed Total Lipedema Care to focus on marketing and providing lipedema treatment. The operation was headquartered at Dr. Schwartz's medical office in Beverly Hills. Dr. Schwartz and his medical corporations shared office space and resources, and both used Dr. Schwartz's computer network to store

patient data, including the data described herein. .

42. On information and belief, at all relevant times, Schwartz Defendants contracted with MEDVA for virtual assistants that assisted with patient scheduling and other matters, and whose employees or agents maintained access to the Schwartz Defendants' patient files and systems.

43. On information and belief, employees or agents of MEDVA held themselves out to patients as employees of the Schwartz Defendants to undertake their work for Schwartz Defendants and served as agents of the Schwartz Defendants at all times. On information and belief, Schwartz Defendants maintained control over MEDVA employees or agents' use of their emails and system access. On information and belief, MEDVA failed to adequately protect against data breaches or unauthorized access to Schwartz Defendants' patient data and EHR systems, including by failing to adequately train its staff on cybersecurity and protection of patient data.

44. On information and belief, at all relevant times, Dr. Schwartz had a contract with ModMed by which ModMed provided health information technology solutions, including the design, security, and maintenance of Dr. Schwartz's cloud-storage systems where patient identifying and medical information was maintained. According to ModMed, that company is "proactive in [its] efforts to maintain EHR information security." Unfortunately, as set forth below, ModMed was not proactive in protecting the class's confidential personal medical information.

45. On information and belief, based on the foregoing, Defendants had custody, control, and/or management of Class Plaintiffs' and other class members personal and medical information, including private and confidential information, and had a duty to safeguard that information.

Dr. Schwartz Maintains Extensive, Confidential Medical Information

46. By virtue of their treatment of Class Plaintiffs and other patients Defendants generated, received, and maintained a large volume of confidential and private information about their patients ("Personal and Medical Information").

47. This Personal and Medical Information includes, without limitation, patients' names, telephone numbers, and home addresses, their ages and dates of birth, their physical characteristics, including height, weight, eye color, and hair color, copies of their driver's licenses and insurance cards, insurance information, *i.e.*, their insurance carriers and types of coverage, payment information, such as credit card information, and medical information, including medical history, conditions, diagnoses, and treatment.

48. Defendants also obtain from patients, generate, and maintain large numbers of photographs and videos depicting patients and their conditions. During the consultation process, Dr. Schwarts and his colleagues regularly ask that patients send in photos depicting their conditions. These photos are frequently nude or partially clothed.

49. In addition, Dr. Schwartz takes extensive photos and videos of patients during the course of treatment. He has an entire room at his surgery center dedicated to taking detailed photos completely documenting patients' physical condition before and after surgery. These photos are also frequently nude or partially clothed.

50. Finally, Dr. Schwartz and his staff film and photograph patients during surgery, ostensibly to allow Dr. Schwartz to document and review the surgery after it is completed. Class Plaintiffs' and other patients' faces are clearly visible in these photographs and video.

51. The photographs and videos are directly connected to Class Plaintiffs' and other patients' names and identifying information on Dr. Schwartz's network.

Defendants Were Obligated to Protect Personal Medical Information

52. Defendants are subject to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for the Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 ("HIPAA"). Among other things, Defendants are and were at all relevant times subject to the *Standards for Privacy of Individually Identifiable*

Health Information (the "Privacy Rule") and the *Security Standards for the Protection of Electronic Protected Health Information* (the "Security Rule"), contained in 45 C.F.R. Parts 160 and 164, Subparts A and C. The Privacy Rule and the Security Rule create nationwide standards for the protection of patient health information.

53. HIPAA required Defendants to "comply with the applicable standards, implementation specifications, and requirements" established under HIPAA "with respect to "electronic protected health information." 45 C.F.R. § 164.302.

54. The Security Rule required Defendants to do all of the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

55. HIPAA further required Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection," 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

56. The California Confidentiality of Medical Information Act, Civil Code § 56, *et seq.* (the "CMIA"), also prohibits the disclosure of patient medical information without authorization. *See* Civ. Code § 56.10. "Medical information" is defined to include (a) individually identifiable information relating to a person's medical history, condition, or treatment, (b) in the possession of or derived from a provider of health care, (c) pertaining to a patient.

57. As "provider[s] of health care" as defined in the CMIA, Civ. Code § 56.05(f), Defendants were required to maintain medical information "in a manner that preserves the confidentiality of the information contained therein."

58. California Health and Safety Code § 1280.15 and 1280.18 require healthcare facilities to safeguard and prevent the unauthorized access of patient medical information.

59. Pursuant to California Civil Code § 1798.81.5(b), any "business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

60. Further, any business that discloses personal information "pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to prevent the personal information from unauthorized access." *Id.*, subd. (c).

61. In addition to the requirements of various statutes and regulations applicable to medical providers and holders of confidential consumer information, Defendants had a common law duty to Class Plaintiffs and other patients to use reasonable care in maintaining, securing, preserving, deleting, and protecting their Personal and Medical Information against the prevalent and well-known threat that it would be compromised, exfiltrated, and misused by unauthorized persons.

62. This duty included, without limitation, a duty to use reasonable security measures consistent with industry standards and requirements, and to ensure that computer systems, networks, and protocols adequately protected the Personal and Medical Information.

Defendants Had Ample Notice of the Risk of Cyberattacks and Industry Standards for Preventing Data Breaches.

63. Defendants were on notice of the risk of hacking in the medical field for years, and in the plastic surgery field in particular. They were also aware, or should have been aware, of the need to use best practices and take reasonable steps to protect sensitive patient information. Defendants brazenly disregarded these standard practices, resulting in the two data breaches alleged herein.

64. For years, the medical community has been the target of hacking due to the perceived value of medical data for extortion and other nefarious purposes. The risk to patient data security posed by this hacking threat has been widely reported and is well known within the medical field.

65. The FBI noted as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their access to obtain" personally identifying information. The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[3]

66. The FBI and U.S. Secret Service have further warned of the risk to the healthcare industry specifically, noting that it is a particular target for cyberattacks. As one report explained, "[e]ntities like smaller municipalities *and hospitals* are attractive … because they often have lesser IT defense and a high incentive to regain access to their data quickly."[4]

67. In 2014, following the hack of Community Health Systems Inc., the FBI warned the medical profession that healthcare firms are targets for hackers. It specifically warned of the risk to patient data: "The FBI has observed malicious actors

[3] Gordon M. Snow Statement, https://archives.fbi.gov/archives/news/testimony/cyber-securitythreats-to-the-financial-sector (last visited January 10, 2024).

[4] Secret Service Warn of Targeted Ransomware, Law360, www.law360.com/articles/1220974/fbi-secretservice-warn-of-targeted-ransomware (last visited January 10, 2024).

targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)." It is well known that patient medical data is highly valuable to hackers for purposes of extortion and ransom, making it a target for data breaches.

68. In 2019, the American Medical Association ("AMA") published a report entitled *Patient Safety: The Importance of Cybersecurity in Healthcare*, warning that cybersecurity "is not just a technical issue, it's a patient safety issue." The report noted that 83% of physicians had experienced some form of cyberattack. Among other risks, the AMA has warned physicians about the risks of ransomware attacks.

69. Since at least 2020, the American Medical Association ("AMA") has maintained a dedicated cybersecurity website, warning doctors and medical groups of the risks of hacking, including the risk to sensitive patient data, and providing industry standard guidelines for information security.

70. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from the previous year.[5]

71. Similarly, since at least 2022, the U.S. Department of Health and Human Services ("DHHS") has maintained its own website on cybersecurity in the healthcare field, again warning of the risks of hacking and unauthorized access to private data.

72. Over the past several years, hackers have begun to focus their efforts on plastic surgery practices due to the sensitive information retained by plastic surgeons. Multiple known and unknown hacker groups, including Hunters International and Kairos, regularly target plastic surgery practices.[6]

---

[5] 2021 Data Breach Annual Report, ITRC, www.wsav.com/wpcontent/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited January 10, 2024).

[6] Some of these groups operate directly, and others offer "Ransomware-as-a-service" in which they license malicious software to third parties for a fee or a share of the ransom obtained through successful breaches. *See* Kurt Baker, *Ransomware as a Service (RaaS) Explained: How It Works & Examples*, CrowdStrike (Jan. 30, 2023).

73. Due to the nature of the data retained by plastic surgeons – *i.e.*, sensitive medical information and private and potentially embarrassing photographs – they are an attractive target. This information is particularly valuable for purposes of sale on the dark web and for extortion attempts against physicians and patients. Frequently these hacks have involved a hacker group gaining access to a surgeon's computer system and exfiltrating large amounts of sensitive patient data, including photographs. Hackers then use this data to attempt to extort the physician and/or patients directly.

74. According to a report from DataBreaches.net, between 2017 and 2023, there were at least a dozen publicly reported successful hacks of plastic surgery practices. Many of these hacks resulted in online data leaks and attempted extortion of surgeons or patients. Several high-profile plastic surgery practices were subject to hacks, such as the 2020 hack of the Hospital Group, and the hacks were widely reported in the media.

75. The American Society of Plastic Surgeons ("ASPS"), of which Dr. Schwartz is a prominent member, has repeatedly warned its membership of the risks of hacking and published guidelines for cybersecurity.

76. Among other things, the ASPS publishes on its website a 2022 report co-authored by the DHHS and the Healthcare & Public Health Sector Coordinating Councils entitled *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* ("DHHS Report"). This report warns of the serious risks of hacking on medical information systems and urges healthcare providers to adopt best practices to protect their systems. It notes, "Given the increasingly sophisticated and widespread nature of cyber-attacks, the health care industry must make cybersecurity a priority and make the investments needed to protect its patients."

77. In June of 2023, the hacking syndicate BlackCat (AlphV), publicly posted that they had hacked the well-known Beverly Hills Plastic Surgery, and "ha[d] lots of PII [patient identifying information] and PHI [protected health information], ***including a lot of pictures of patients that they would not want out there***." This hack

was also publicly reported.

78. In the same timeframe, another well-known plastic surgeon in the Los Angeles area was hacked. When the surgeon refused to pay a $2.5 million ransom, the hackers began leaking nude photos of patients along with their personal identifying information and threatened to leak more until the ransom was paid. The hackers also directly contacted patients and demanded $800,000 to remove their photos from a hacker website. This hack was also publicly reported.

79. On July 6, 2023, the ASPS sent an alert to its membership, entitled *Notice of ransomware scam targeting plastic surgeons*, about the risk of ransomware "phishing" attacks. The alert warned that hackers had targeted plastic surgeons, and having gained access to the surgeons' systems, "***comb[] the surgeon's network for patient data and photos***. This then leads to an extortion attempt to release that data."

80. The hacking threat against plastic surgeons has become so significant that in October of 2023, the FBI issued a Public Service Announcement, entitled *Cybercriminals are Targeting Plastic Surgery Offices and Patients*, Alert Number: I-101723-PSA, warning surgeons of the risk of hacking. The Public Service Announcement again warned that cybercriminals were actively targeting plastic surgery offices "*to harvest personally identifiable information and sensitive medical records, **to include sensitive photographs*** in some instances."

81. The announcement explained the process of these hacks, including:

a. "Data Harvesting," including "harvest[ing] electronically protected health information (ePHI), which includes sensitive information and photographs";

b. "Data Enhancement," using publicly available information, such as social media, to gather additional information about patients to use in extortion; and

c. "Extortion," demanding money from surgeons and patients to prevent disclosure of the sensitive data.

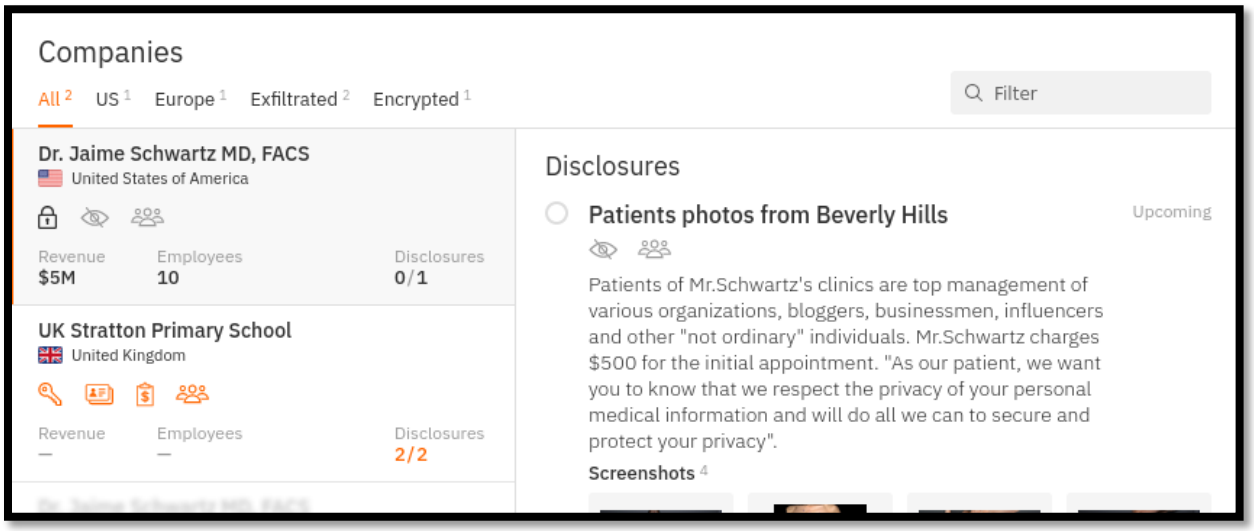
82. The announcement noted that, "[t]o exert pressure on victims for extortion payments, cybercriminals share the sensitive ePHI to victims' friends,

family, or colleagues, and create public-facing websites with the data. Cybercriminals tell victims they will remove and stop sharing their ePHI only if an extortion payment is made."

83. On October 19, 2023, the ASPS reposted the FBI Public Service Announcement on its website.

October 2023—The First Hack and Failed Response

84. On information and belief, in September or October 2023, the hacker group Hunters International successfully hacked Dr. Schwartz's network (the "First Hack"). The group took credit for the successful hack on the dark web:



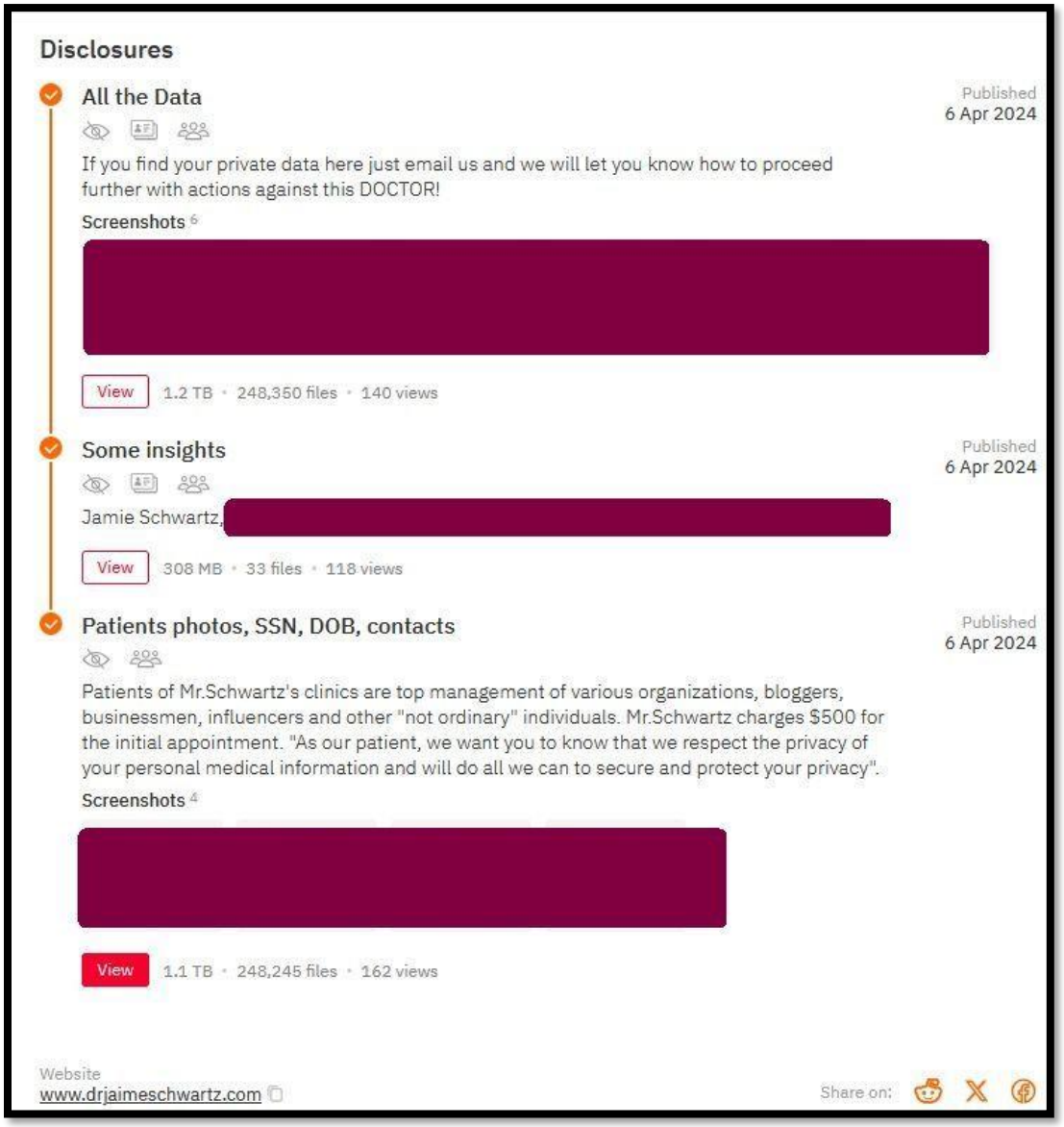
85. According to its dark web posting, Hunters International had exfiltrated 1.1 terabytes of data from that system, consisting of 248,245 files. Based on publicly available data, the dark web posting included four patient photos, including one nude photo with the patient's face visible. The hackers claimed that they had hacked Dr. Schwartz's system in September of 2023.

86. On November 11, 2023, Hunters International updated their dark web posting by listing patient data and included the following note to Dr. Schwartz:

> Seems like you don't want to protect your data at all. More than 30 days had passed already since your network has been breached. You have been provided with everything you have asked about: sample of files, decryption tool demonstration, filetree, personal details. But you keep begging for proofs. This is not the way we going to make business with you. Maybe

you will do us a favor and transfer half of the money to prove that you can pay for your data? That would be fair, we guess. **Nevertheless, we will start deploying a little piece of your data everyweek, until all of your data will be shared this way. Starting today. You still have an option to pay for your data, until sharing is finished.**

87. In April 2024, Hunters International reposted its dark web listing, this time adding nude photos of patients, and advising, "If you find your private data here just email us and we will let you know how to proceed further with actions against this DOCTOR!"



88. Defendants did not notify patients of the September/October 2023 attack.

Dr. Schwartz unequivocally refused to pay ransom. On information and belief, Defendants also failed to provide required notices to the California Attorney General or the DHHS.

89. Instead, when a small number of patients contacted Dr. Schwartz after the First Hack was reported online, he and his staff attempted to minimize the data breach by falsely claiming that it affected only a small number of patients and that other patients' records were secure. Dr. Schwartz and his colleagues continued to assure patients (falsely) that their data was not compromised and was secure.

90. Eventually, Hunters International posted all or substantially all of the exfiltrated data on its dark web "leak" site, organized by client name.

March 2024—The Second Hack

91. Despite hackers compromising Dr. Schwartz's system and attempting to extort him, Defendants still failed to implement reasonable security protocols.

92. In early 2024, Dr. Schwartz's system was hacked a second time (the "Second Hack"; collectively with the First Hack, "Data Breaches") by a different hacker group, operating under the name "Boobs & Pussies."

93. Dr. Schwartz claims that he first learned of this hack in late June 2024 but, on information and belief, he learned of the second hack much earlier.

94. It is unclear how long the system had been compromised before Dr. Schwartz purportedly "discovered" the Second Hack. According to the Hacker Site – a public, "clear web" site[7] posted by the hackers – they successfully compromised Dr. Schwartz's system in March of 2024.

95. The hackers again obtained large amounts of sensitive patient data, including the data of the Class Plaintiffs. On information and belief, the hackers exfiltrated Personal and Medical Information of at least hundreds of patients.

[7] The "clear web" or "surface web" refers to the publicly accessible internet, indexed by standard search engines, such as Google. It is distinguished from the "dark web" which must be accessed through specialized software.

96. This data included patient's full names, identifying information, home addresses, dates of birth, and physical data, as well as insurance information and payment information regarding procedures not covered by insurance. According to Dr. Schwartz's belated notice of the data breach, the affected data also included medical information and prescription medications. Most disturbingly, it included nude and partially clothed photographs and videos, including photographs during surgery.

97. On or about December 16, 2024, the hackers posted the Hacker Website, announcing the hack and disclosing that Dr. Schwartz had refused to address the incident for months. The website includes extremely sensitive data, including personally identifying information of patients and nude photos taken during surgery. The hackers also threaten on the website to continue releasing information and photos of additional patients if Dr. Schwartz does not contact them.

98. To date, the hackers have published sensitive personal information of 79 patients, organized by name and data of birth. The files include headshots of the victims, full, unredacted copies of their drivers' licenses and insurance cards, and nude and partially clothed photos, depicting their medical conditions and surgeries. Some of the photos appear to have been taken while patients were unconscious and undergoing surgery, reflecting surgical incisions and sutures.

99. The hackers have continued posting patient data and images online since the filing of this action.

100. Once again, on information and belief, Defendants failed to take reasonable steps to secure their shared system and failed to respond in an appropriate manner to the second hack as required by law.

Defendants' Untimely and Incomplete Disclosure

101. In January of 2025, Dr. Schwartz sent certain patients, including Class Plaintiffs, a Notice of Data Security Incident (the "Data Breach Notice"). In it, he notified patients as follows:

Our office discovered on June 27, 2024, that an unauthorized third party

> utilized a third-party vendor's credentials to access the practice's medical billing and practice management system. Upon discovering the incident, we engaged a specialized third-party forensic incident response firm to conduct a forensic investigation and determine the extent of the compromise. The investigation determined that data was acquired without authorization. After electronic discovery, which concluded on January 2, 2025, it was determined that some of your personal information was present in the impacted data set. We then took steps to notify you of the incident as quickly as possible.

102. In the Data Breach Notice, Dr. Schwartz also claimed that he was "looking into enhancements to prevent a similar incident." He also recognized the actual, imminent harm and injury to patients, noting that victims are encouraged to "remain vigilant and monitor your accounts for suspicious activity."

103. He continued to assure patients that he was taking their privacy seriously, noting "[p]lease be assured that we take the privacy and security of all personal information …very seriously," and that data security "is among our highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care."

104. Defendants failed to timely notify the California Attorney General or the DHHS as required by law. Dr. Schwartz notified the California Attorney General only after the filing of this lawsuit and, on information and belief, has not notified the DHHS.

105. On information and belief, Defendants still have not notified all affected patients whose Personal and Medical Information was leaked in the Second Hack.

106. Because Defendants have not yet made a full or transparent disclosure of the hack, significant questions remain about the nature and scope of the hack and the types and amounts of data that have been compromised. Plaintiffs are informed and believe, however, that the hackers gained access to, viewed, and/or copied substantially all of the patient data on Dr. Schwartz's system.

Defendants Negligently Maintained Dr. Schwartz's Systems

107. The Data Breaches were caused by Defendants' negligence in retaining

patient data and failing to secure the network and computer systems, which allowed malicious actors to gain access to those systems and to access and exfiltrate unencrypted Personal and Medical Information.

108. On information and belief, the malicious actors were able to access confidential Personal and Medical Information due to a series of negligent failures in Defendants' cybersecurity procedures, including a defectively designed and secured data storage, insufficient training, and negligent conduct allowing access to the network by unauthorized individuals.

Prevailing Standards for Protection of Sensitive Patient Data

109. Governmental agencies, industry organizations, and technology companies have established a set of basic cybersecurity standards to minimize the risk of hacking and access to unencrypted patient or customer data.

110. For example, the DHHS Report provides the following basic cybersecurity protocols for the medical industry, among others:

a. securing email accounts;

b. installing and maintaining spam/anti-virus software solutions;

c. using multi-factor authentication (MFA);

d. correctly configuring security settings;

e. training employees on cybersecurity;

f. limiting user access to administrative accounts so that administrative accounts are used only for essential purposes;

g. utilizing encryption on user devices;

h. enabling network firewalls;

i. utilizing MFA for access to connected devices;

j. maintaining unique user accounts and tailoring each user's access to essential functionality and data;

k. using encrypted storage media and devices for sensitive information;

l. controlling access to sensitive and highly sensitive data within the network, including placing more sensitive data in restricted zones that are more difficult to access;

m. limiting third-party vendor access to sensitive data;

n. establishing and enforcing network "traffic" restrictions;

o. monitoring network activity and maintaining an audit trial, and

p. monitoring and patching vulnerabilities and keeping software updated.

111. The FBI recommends the following security measures, among others:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when

necessary.

h. Configure access controls-including file, directory, and network share permissions-with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

112. The United States Cybersecurity & Infrastructure Security Agency recommends the following protective measures, among others:

a. Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....

b. Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website

or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....

c. Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d. Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it....

e. Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f. Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques….

g. Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic...

113. The Federal Trade Commission ("FTC") urges businesses to adopt appropriate cybersecurity measures, noting the need for data security to be factored into all business decision-making. To that end, the FTC has issued numerous guidelines for data security. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, with the following guidelines for fundamental data security principles and practices:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of sensitive information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

114. The FTC also recommends that businesses watch for large volumes of data being transmitted from their systems and have a response plan ready in the event of a breach.

115. Finally, the FTC recommends that companies not maintain information for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

116. HIPAA also establishes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.

117. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.

118. In addition to standards and guidelines established by statute, regulation, and government agencies, well-established industry standards exist for cybersecurity. As noted above, experts studying cybersecurity routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the information they possess.

119. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which

employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

120. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

121. Consistent with established industry standards, the Microsoft Threat Protection Intelligence Team, an industry leader in cybersecurity, recommends the following practices:

a. Secure internet-facing assets;

b. Apply latest security updates;

c. Use threat and vulnerability management;

d. Perform regular audits;

e. Remove privileged credentials

f. Thoroughly investigate and remediate alerts;

g. Prioritize and treat commodity malware infections as potential full compromise;

h. Include IT Pros in security discussions

i. Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

j. Build credential hygiene

k. Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

l. Apply principle of least-privilege;

m. Monitor for adversarial activities;

n. Hunt for brute force attempts;

o. Monitor for cleanup of Event Logs;

p. Analyze logon events;

q. Harden infrastructure;

r. Use Windows Defender Firewall;

s. Enable tamper protection;

t. Enable cloud-delivered protection;

u. Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

122. In addition, industry practice incorporates the NIST Cybersecurity Framework, Version 2.0 (including without limitation, PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

Defendants' Failure to Implement Reasonable Protections

123. Defendants failed to implement and maintain reasonably adequate cybersecurity protocols, which failure allowed and exacerbated the Data Breaches. On information and belief, their negligent failures to protect patient data included, without limitation, the following.

124. As set forth in more detail below, Defendants failed to properly design their data systems (including those systems provided by ModMed), adopt and implement standard cybersecurity protections, ensure the security of their network, and adequately train their staff and vendors (including Medva and the virtual assistants it provided). In doing so, Defendants violated both statutory law (including HIPAA), regulations, and the above-described industrywide minimum standards for cybersecurity.

125. Defendants failed to store highly sensitive patient data in appropriately secured parts of their network consistent with the sensitivity of the data and, on

information and belief, stored patient data in an unencrypted format or with inadequate encryption in place.

126. Plaintiffs are informed and believe that ModMed was responsible for hosting sensitive patient data, including designing and implementing the data storage structure used for the Schwartz Defendants' patient data. On information and believe, ModMed failed to competently design its system such that extremely sensitive patient data was adequately segregated or secured so that malicious actors gaining access to the Schwartz Defendants' system could not access and exfiltrate that data.

127. In addition, Defendants allowed sensitive patient data, including photographs, videos, and medical information, to be stored on unused and obsolete systems, and outside of a secured network, and allowed those systems to remain accessible after they were no longer in use.

128. Defendants failed to adequately secure patient files to prevent them from being accessible over the internet.

129. Defendants failed to properly manage access to their system, including failing to implement appropriate multi-factor authentication for staff and vendors, gave staff and vendors access to information that was not necessary to perform their functions, failed to enforce appropriate credential hygiene – *e.g.*, regular password changes –, and failed to ensure that users had appropriate, strong passwords.

130. Defendants also failed to adequately restrict user access to network resources and data for which those users had no legitimate need and stored sensitive patient data that allowed access by user accounts without a legitimate need for access. For example, Plaintiffs are informed and believe, that the Schwartz Defendants and Medva allowed Medva virtual assistants extensive access to patient files, which was unnecessary for them to perform their assigned tasks.

131. Defendants failed to secure network-connected devices, including connected medical devices, in a manner reasonably designed to prevent intrusion.

132. Defendants failed to adequately train their staff, including virtual

assistants provided by Medva, to avoid "phishing" and other social-engineering attacks, failed to use due care in selecting and supervising third-party vendors, and failed to reasonably ensure that vendors with access to sensitive patient data were appropriately retained and maintained secure access credentials.

133. Defendants utilized third-party applications, such as patient-communication platforms, to store and/or access sensitive data, without adequate security measures in place to ensure that such platforms were not subject to cyberattack.

134. Defendants failed to adequately monitor network traffic or suspicious network activity as necessary to prevent or promptly discovery malicious activity, and failed to implement appropriate network "traffic" controls to prevent the exfiltration of large amounts of data. Defendants also failed to use appropriate anti-malware software and firewalls to prevent and detect suspicious network activity and failed to appropriately train staff to detect suspicious activity and avoid or mitigate the risk of malicious activity on the network.

Defendants' Negligent Security Allows the Cyberattacks

135. The negligence outlined above allowed the Data Breaches and proximately caused the harm to Plaintiffs and Class Members alleged herein.

136. While there have been conflicting accounts of the Data Breaches, Plaintiffs are informed and believe that the malicious actors gained access initially through a common "phishing" technique. The hackers emailed a mislabeled file to Dr. Schwartz's staff, purporting to be a patient file, but containing malicious code. On information and belief, a Medva virtual assistant holding himself or herself out as an employee of Dr. Schwartz opened the file, allowing the hackers access.

137. Had the Schwartz Defendants' staff, including the Medva virtual assistants, been adequately trained, they would have recognized the email as suspicious, and would have known not to open the attached file.

138. The malicious actors then used the compromised user account to gain

broad access to the Schwartz Defendants' network, including highly sensitive patient data. While compromising a staff account gave the hackers initial access, it was only through the defective design, management, and security of Defendnats' network that the hackers were able to gain access to and exfiltrate sensitive patient files.

139. Had the network been adequately designed and secured, the hackers would not have been able to use the initial access gained through a general staff account to access highly confidential patient data. For example, appropriate user access controls would have limited access to sensitive data to those staff members with a legitimate need to access it, such that compromising a staff account would not have given hackers access. Further, additional encryption of highly sensitive data, would also have prevented hackers from accessing sensitive patient data.

140. These security measures were industry standard in the healthcare industry at the time and were not implemented by Defendants, leading to the Data Breaches.

The Impact of the Cyberattacks on Class Plaintiffs

Jane Doe A

141. Plaintiff Jane Doe A is a former patient of Total Lipedema Care and a Data Breach Victim. Plaintiff contacted Dr. Schwartz and he refused to confirm whether Plaintiff's information was compromised, despite the fact Plaintiff received an alert that her Sensitive Information has been posted on the Dark Web.

142. Plaintiff saw Dr. Schwartz in 2019 for consultations. Had Jane Doe A known that Dr. Schwartz did not have appropriate procedures in place to protect her sensitive information, and was negligently handling sensitive patient data, she would not have sought treatment or consultation with Defendants.

143. As a condition of treatment with Dr. Jaime Schwartz and Total Lipedema Care, Plaintiff provided Defendants with her Personal and Medical Information, including her full name, address, phone number, Driver's License (copied), insurance information, payment information, and medical records. Additionally, Plaintiff was required to send nude and semi-nude photos to Defendants for consultation purposes,

and Dr. Schwartz also photographed Plaintiff.

144. Defendants used that Personal and Medical Information to facilitate their treatment of Plaintiff and required Plaintiff to provide that Personal and Medical Information to obtain treatment and care.

145. When Plaintiff provided her Personal and Medical Information to Defendants, she trusted that they would use reasonable measures to protect it according to state and federal law. She would not have provided her Personal and Medical Information to Defendants, or sought medical treatment from Defendants, if she knew about Defendants' lax cybersecurity policies.

146. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breaches' effects by entirely failing to inform Plaintiff of Data Breaches.

147. As a result of their inadequate cybersecurity, Defendants exposed Plaintiff's Personal and Medical Information and highly private photographs to theft by cybercriminals and sale on the Dark Web. Indeed, Plaintiff received an alert that her personal identifying information has been posted to the Dark Web.

148. Plaintiff suffered actual injury from the exposure of her Personal and Medical Information—which violates her rights to privacy.

149. Worse, Plaintiff has been directly contacted by cybercriminals by telephone multiple times on June 30, 2025, at 12:14 a.m., 12:15 a.m., and 12:30 a.m., who were attempting to hack Plaintiff's Google account, which is connected to the same email address Plaintiff provided to Dr. Schwartz's office.

150. Because of the Data Breach, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and criminals.

151. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach. Plaintiff originally spent over 40 hours researching

the Data Breach, filing numerous reports with the U.S. Internet Crimes Complaint Center ("IC3"), IC3.gov, communicating with the FBI and the Beverly Hills Police Department, and speaking with and supporting other victims.

152. Plaintiff continues to spend time attempting to mitigate her damages by self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. She also spent time placing a credit freeze on her accounts, and researching identity theft monitoring and data removal services. This time has been lost forever and cannot be recaptured. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from additional identity theft.

153. In response to the Data Breaches and telephone calls, Plaintiff purchased identity theft monitoring services and data removal services at her own expense.

154. Plaintiff fears for her personal financial security and uncertainty over whether her data and images of her will be posted on the Hacker Website or elsewhere, and whether that data will be used for nefarious purposes, including identity theft.

155. Plaintiff is suffering from insomnia, nausea, fatigue, and panic attacks. Plaintiff has and is experiencing feelings of fear, embarrassment, shock, anxiety, and depression as a result of her private data and photographs being compromised. Plaintiff is specifically experiencing fear of being recognized, fear of opening email or electronic communications, and is generally unable to concentrate. Plaintiff's experiences go far beyond mere worry or inconvenience; they are exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

156. Plaintiff has suffered actual injury in the form of lost money and damages to and diminution in the value of their Personal and Medical Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breaches.

157. Plaintiff does not recall ever learning that her private medical information and photographs were compromised in a data breach incident, other than the Data

Breaches at issue in this case.

158. Plaintiff has a continuing interest in ensuring that her Personal and Medical Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Jane Doe B

159. Plaintiff Jane Doe B is a former patient of Total Lipedema Care and a Data Breach Victim, having received Notice of the Second Data Breach from Dr. Schwartz.

160. Plaintiff saw one of Dr. Schwartz's employees or associates, Dr. Herbst, in January 2024 and then saw Dr. Schwartz in February 2024, for consultations related to Dercum's Disease and Lipedema, painful and potentially disfiguring conditions. Jane Doe A paid for these consultations out of pocket. As a condition of receiving treatment from Dr. Schwartz and Total Lipedema Care, Plaintiff provided Defendants with her Personal and Medical Information, including her full name, address, phone number, Military identification card, Driver's License (copied), insurance information, payment information, and medical records. Additionally, Plaintiff was required to send semi-nude photos to Defendants for consultation purposes.

161. Defendants used that Personal and Medical Information to facilitate their treatment of Plaintiff and required Plaintiff to provide that Personal and Medical Information to obtain treatment and care.

162. When Plaintiff provided her Personal and Medical Information to Defendants, she trusted that they would use reasonable measures to protect it according to state and federal law. She would not have provided her Personal and Medical Information or highly sensitive photographs to Defendants, or sought and paid for medical treatment from Defendants, if she knew about Defendants lax cybersecurity policies.

163. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breaches' effects by failing to notify Plaintiff of the Second Hack

within a reasonable time.

164. As a result of their negligent cybersecurity practices, Defendants exposed Plaintiff's Personal and Medical Information and highly private photographs for theft by cybercriminals and sale on the Dark Web.

165. Plaintiff suffered actual injury from the exposure of her Personal and Medical Information and highly private photographs—which violates her rights to privacy. Indeed, Plaintiff's Personal and Medical Information has already been posted on the Hacker Website, including at minimum Plaintiff's Driver's License (front and back), Military Identification card (front and back), and semi-nude photos. A link to download Plaintiff's complete patient file is also available on the Hacker Website.

166. Although Plaintiff spent money signing up for a service that helps individuals remove their personal information from the internet, when Plaintiff's full name is entered into Google, the search engine returns a link to the Hacker Website, which contains her patient file, including the photographs.

167. Plaintiff is a victim of identity theft and fraud. Following the Second Hack, Plaintiff experience fraudulent charges on her credit card accounts.

168. Because of the Data Breaches, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal and Medical Information being placed in the hands of unauthorized third parties and criminals. This injury is worsened by Defendants' failure to inform Plaintiff about the Second Hack in a timely fashion.

169. As a result of the Data Breaches, Plaintiff spent time dealing with the consequences. To date, Plaintiff has spent numerous hours verifying the legitimacy of the Data Breach Notice, and attempting to mitigate her damages by self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff also contacted Google multiple times to try to get her name removed from their index, so the semi-nude photos of her posted to the Hacker Website are not returned in response to the query. This time has been lost forever and cannot be recaptured.

Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from additional identity theft.

170. Plaintiff fears for her personal financial security and uncertainty over whether more of her data and additional semi-nude images of her will be posted on the Hacker Website or elsewhere, and whether that data will continue to be used for nefarious purposes, including identity theft. Plaintiff lives in constant fear of someone googling her name and finding semi-nude images of her online, or someone stealing her identity.

171. Plaintiff has and is experiencing feelings of fear, embarrassment, humiliation, shock, anxiety, and insomnia as a result of her private data and photographs being compromised. Plaintiff is further experiencing a strong, overwhelming feeling of impending doom, and no longer trusts doctors and medical professionals. Plaintiff's experiences go far beyond allegations of mere worry or inconvenience; they are exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

172. Plaintiff has also suffered actual injury in the form of damages to and diminution in the value of her Personal and Medical Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

173. Plaintiff does not recall ever learning that her private photographs were compromised in a data breach incident, other than the Data Breaches. Plaintiff has a continuing interest in ensuring that her Personal and Medical Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Jane Doe C

174. Plaintiff is a former patient of Total Lipedema Care and a Data Breach Victim. Although her Personal and Medical Information, including highly private photographs, has been posted on the Hacker Website, Plaintiff is still awaiting formal

notice of the Data Breaches from Defendants.

175. Plaintiff saw Dr. Schwartz in 2023 for consultations related to Lipedema treatment, a painful and potentially disfiguring condition.

176. As a condition of treatment with Dr. Schwartz and Total Lipedema Care, Plaintiff provided Defendants with her Personal and Medical Information, including her full name, address, phone number, Driver's License (copied), and insurance information. Additionally, Plaintiff was required to send semi-nude photos to Defendants for consultation purposes.

177. Defendants used that Personal and Medical Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Sensitive Information to obtain treatment and care.

178. When Plaintiff provided her Personal and Medical Information to Defendants, she trusted that they would use reasonable measures to protect it according to state and federal law. She would not have provided her Personal and Medical Information or highly sensitive photographs to Defendants, or sought medical treatment from Defendants, if she knew about Defendants' lax cybersecurity policies.

179. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breaches' effects by entirely failing to inform Plaintiff of the Data Breaches, despite the fact her data and photographs have been posted on the Hacker Website.

180. As a result of their inadequate cybersecurity, Defendants exposed Plaintiff's Personal and Medical Information and highly private photographs for theft by cybercriminals and sale on the Dark Web.

181. Plaintiff suffered actual injury from the exposure of her Personal and Medical Information and highly private photographs—which violates her rights to privacy. Indeed, Plaintiff's Sensitive Information has already been posted on the Hacker Website, including at minimum Plaintiff's Driver's License (front and back), health insurance card, and semi-nude photos. A link to download Plaintiff's file is also

available on the Hacker Website.

182. Additionally, when Plaintiff's full name is entered into Google, the search engine returns a link to the Hacker Website, which contains her file, including the photographs.

183. Plaintiff has been directly contacted by cybercriminals multiple times, who have tried and are trying to extort her.

184. Because of the Data Breaches, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal and Medical Information being placed in the hands of unauthorized third parties and criminals.

185. As a result of the Data Breaches, Plaintiff spent time dealing with the consequences of the Data Breach. To date, Plaintiff estimates that she has spent at least 60-80 hours verifying the legitimacy of the Data Breaches, communicating with other victims, attempting to mitigate her damages by placing a credit freeze on her accounts, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from additional identity theft.

186. Plaintiff also purchased identity theft protection software at her own expense in response to the Data Breaches.

187. Plaintiff fears for her personal financial security and uncertainty over whether more of her data and additional images of her will be posted on the Hacker Website or elsewhere, and whether that data will be used for nefarious purposes, including identity theft. Plaintiff lives in constant fear of someone googling her name and finding semi-nude images of her online, or someone stealing her identity.

188. Plaintiff is suffering from insomnia, nausea, headaches, and fatigue. She is overwhelmed, exhausted, and withdrawn to the point she no longer communicates regularly with her friends and family. Plaintiff has and is experiencing feelings of fear,

embarrassment, humiliation, shock, anxiety, and depression as a result of her private data and photographs being compromised. Plaintiff is further experiencing a strong, overwhelming feeling of impending doom, and no longer trusts doctors and medical professionals. Plaintiff also fears opening email or electronic communications and is generally unable to concentrate.

189. Plaintiff has and continues to confer with medical professionals about the symptoms she is suffering as a result of Data Breaches, and how the Data Breaches have generally impacted her overall health. Plaintiff's experiences go far beyond allegations of mere worry or inconvenience; they are exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

190. Plaintiff has also suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

191. Plaintiff does not recall ever learning that her private medical information and photographs were compromised in a data breach incident, prior to the data breaches at issue in this case.

192. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Jane Doe D

193. Plaintiff Jane Doe D is a former patient of Total Lipedema Care and a Data Breach Victim. Although her Personal and Medical Information, including highly private photographs, has been posted on the Hacker Website since at least December 24, 2024, Plaintiff is still awaiting formal notice of the Data Breach from Defendants.

194. Plaintiff saw Dr. Schwartz from May 2021 to late 2024 for consultations related to Lipedema treatment, a painful and potentially disfiguring condition. Plaintiff

paid out of pocket for these consultations. Had Plaintiff known of Defendants' lax and negligent policies for maintaining the security of her sensitive information, Plaintiff would not have consulted with Defendants or paid them.

195. As a condition of treatment with Dr. Schwartz and Total Lipedema Care, Plaintiff provided Defendants with her Personal and Medical Information, including her full name, address, phone number, Driver's License (copied), insurance information, payment information, and medical records. Additionally, Plaintiff was required to send nude and semi-nude photos to Defendants for consultation purposes.

196. Defendants used that Personal and Medical Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Personal and Medical Information to obtain treatment and care.

197. When Plaintiff provided her Personal and Medical Information to Defendants, she trusted that they would use reasonable measures to protect it according to state and federal law. She would not have provided her Personal and Medical Information or highly sensitive photographs to Defendants, or sought medical treatment from Defendants, if she knew about Defendants lax cybersecurity policies.

198. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breaches' effects by entirely failing to inform her of the Data Breaches, despite the fact her data and photographs have been posted on the Hacker Website since the first batch of data and photographs were posted.

199. As a result of their inadequate cybersecurity, Defendants exposed Plaintiff's Personal and Medical Information and highly private photographs for theft by cybercriminals and sale on the Dark Web.

200. Plaintiff suffered actual injury from the exposure of her Personal and Medical Information and highly private photographs—which violates her rights to privacy. Indeed, Plaintiff's Personal and Medical Information has already been posted on the Hacker Website, including at minimum Plaintiff's Driver's License (front and back), health insurance card, and semi-nude photos. A link to download Plaintiff's

complete patient file is also available on the Hacker Website.

201. Additionally, when Plaintiff's full name is entered into Google, the search engine shows a thumbnail image of her face from one of her medical photographs and returns a link to the Hacker Website, which contains her complete patient file, including the photographs. Due to the nature of Plaintiff's profession, her name is frequently googled, so she is working diligently to change her name. Because her name is associated with her professional work on numerous websites and searchable databases, the process of the name change has taken more than 25 hours and will require more effort from Plaintiff and others at her place of work. The name change also has significant negative repercussions in her field where name recognition is important.

202. Worse, in December 2024, cybercriminals telephoned Plaintiff and told her they had her highly private photographs. On July 8 and July 9, 2025, the same or other cybercriminals emailed Plaintiff copies of photographs she provided to Defendants.

203. Additionally, Plaintiff recently discovered that her medical records are accessible through an unsecure and easily hackable mobile application, APPatient, which is used by the Schwartz Defendants to store and manage patient medical information.

204. For example, Plaintiff was able to reset her password on APPatient by simply selecting the "reset password" option and directing the application to send a reset link to her email address—an email address that has been previously compromised in the Data Breaches at issue here and is posted on the Hacker website.

205. Upon clicking the link, Plaintiff was able to reset the password and gain full access to her medical records without encountering any additional security measures. The accessed records included highly sensitive personal information such as insurance details, contact information, medical history, mental health records, and histories of sexual abuse and substance use. At no point was Plaintiff required to

complete any form of two-factor authentication or similar security verification to access this highly sensitive information.

206. Furthermore, Plaintiff could not identify any available means within the application to enable enhanced security measures, remove her information, or delete her account. The continued insecurity of Plaintiff's sensitive data despite the Data Breaches, combined with her inability to take any action to further protect it, has significantly exacerbated her emotional distress.

207. Because of the Data Breaches, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and criminals. She recently discovered that her PayPal account, which was linked to the personally identifying information available on the Hacker Website, was breached. Anyone who gained access to the PayPal account would also have access to her bank account information, debit card, and credit cards.

208. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach. To date, Plaintiff estimates that Plaintiff has spent at least 80 hours verifying the legitimacy of the Data Breaches, attempting to mitigate her damages by changing her professional name, placing a credit freeze on her accounts, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, cancelling her credit and debit cards, and deleting her personal email account. Additionally, whenever Plaintiff receives medical information from any of her doctors, she does extensive research to make sure the contact is legitimate. This time has been lost forever and cannot be recaptured. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from additional identity theft and plans to change her personal phone number soon.

209. Plaintiff purchased her own identity protection service, costing $99/year.

210. Plaintiff fears for her personal financial security and uncertainty over whether more of her data and additional nude images of her will be posted on the

Hacker Website or elsewhere, and whether that data will be used for nefarious purposes, including identity theft. Plaintiff lives in constant fear of someone googling her name and finding nude or semi-nude images of her online, or someone stealing her identity.

211. For months following her discovery of the Data Breach, Plaintiff suffered from acute symptoms of depression that interfered with her ability to perform her job and care for her family and herself. Plaintiff continues to suffer from PTSD, insomnia, nausea, fatigue, and panic attacks. She has lost weight, and her lipedema symptoms have worsened. She has seen a doctor, an acupuncturist, and therapist because of the symptoms she is suffering from the Data Breach.

212. Plaintiff has and is experiencing feelings of fear, embarrassment, shock, and anxiety as a result of her private data and photographs being compromised. Plaintiff is specifically experiencing fear of being recognized, fear of opening email or electronic communications, and substantial distrust of doctors and medical professionals. Whenever any of her doctors send her medical information via email, she does extensive research to make sure the contact is legitimate. The stress of the Data Breaches have also caused Plaintiff to miss work and important deadlines, prompting her employer to provide her with negative feedback in her annual evaluations.

213. Plaintiff has and continues to confer with medical professionals about the symptoms she is suffering as a result of the Data Breaches, and how the Data Breaches have generally impacted her overall health. Plaintiff's experiences go far beyond allegations of mere worry or inconvenience; they are exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

214. Plaintiff has also suffered actual injury in the form of damages to and diminution in the value of her Personal and Medical Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breaches.

215. Plaintiff does not recall ever learning that her private photographs were compromised in a data breach incident, other than the Data Breaches.

216. Plaintiff has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession and is stored on the unsecure and easily hackable mobile app APPatient, is protected, and safeguarded from future breaches.

Jane Doe E

217. Plaintiff Jane Doe E is a former patient of Total Lipedema Care and a Data Breach Victim. Although her Personal and Medical Information, including highly private photographs, has been posted on the Hacker Website, Plaintiff did not receive notice of the Second Hack until she called Defendants and demanded they send her a notice, which she finally received in March 2025.

218. Plaintiff saw Dr. Schwartz's employee or associate, Dr. Herbst, in June 2021 and then saw Dr. Schwartz in November 2023 for consultations related to Lipedema treatment. Plaintiff paid out of pocket for these consultations. Had she known of Defendants' negligent handling of sensitive patient information, she would not have consulted with Defendants or paid them.

219. As a condition of treatment with Dr. Schwartz and Total Lipedema Care, Plaintiff provided Defendants with her Personal and Medical Information, including her full name, address, phone number, Driver's License (copied), insurance information, payment information, and medical records. Additionally, Plaintiff was required to send semi-nude photos to Defendants for consultation purposes.

220. Defendants used that Personal and Medical Information to facilitate its treatment of Plaintiff and required Plaintiff to provide that Personal and Medical Information to obtain treatment and care.

221. When Plaintiff provided her Personal and Medical Information to Defendants, she trusted that they would use reasonable measures to protect it according to state and federal law. She would not have provided her Personal and

Medical Information to Defendants, or sought medical treatment from Defendants, if she knew about Defendants' lax cybersecurity policies.

222. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breaches' effects by entirely failing to inform Plaintiff of First Hack, and by failing to notify Plaintiff of the Second Hack within a reasonable time. Indeed, Defendants entirely failed to inform Plaintiff of the First Data Breach and did not send her a Data Breach Notice relating to the Second Data Breach until nearly a year after that breach occurred, and after Plaintiff demanded notice.

223. As a result of their inadequate cybersecurity, Defendants exposed Plaintiff's Personal and Medical Information and highly private photographs for theft by cybercriminals and sale on the Dark Web. Indeed, Plaintiff received an alert that her personal identifying information has been posted to the Dark Web.

224. Plaintiff suffered actual injury from the exposure of her Personal and Medical Information—which violates her rights to privacy. Indeed, Plaintiff's Personal and Medical Information has already been posted on the Hacker Website, including at minimum Plaintiff's Driver's License (front and back), health insurance card, and semi-nude photos. A link to download Plaintiff's complete patient file is also available on the Hacker Website.

225. Additionally, when Plaintiff's full name is entered into Google, the search engine returns a link to the Hacker Website, which contains her patient file, including the photographs.

226. Worse, Plaintiff has been directly contacted by cybercriminals multiple times, who have tried and are trying to extort her.

227. Because of the Data Breaches, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Personal and Medical Information being placed in the hands of unauthorized third parties and criminals.

228. As a result of the Data Breaches, Plaintiff spent time dealing with the

consequences. Plaintiff originally spent over 80 hours researching the Data Breaches and verifying the legitimacy of the Data Breach Notice, and now Plaintiff spends approximately 1 to 3 hours per week attempting to mitigate her damages self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. She also spent time placing a credit freeze on her accounts. This time has been lost forever and cannot be recaptured. Plaintiff will continue to spend considerable time and effort monitoring her accounts to protect herself from additional identity theft.

229. Plaintiff also requested that Defendants provide her with a credit monitor service, and initially Defendants agreed to cover the costs. However, they subsequently declined to provide Plaintiff with any details regarding the sign-up process and did not assure her that they would reimburse if should she independently enroll in credit monitoring services. Plaintiff now receives credit monitoring services through her bank and pays an additional $20.00 a month for title monitoring services.

230. Plaintiff fears for her personal financial security and uncertainty over whether more of her data and additional images of her will be posted on the Hacker Website or elsewhere, and whether that data will be used for nefarious purposes, including identity theft. Plaintiff lives in constant fear of someone googling her name and finding nude or semi-nude images of her online, or someone stealing her identity.

231. Plaintiff is suffering from insomnia, headaches, fatigue and panic attacks. Plaintiff has and is experiencing feelings of fear, embarrassment, humiliation, shock, anxiety, and depression as a result of her private data and photographs being compromised. Plaintiff is specifically experiencing fear of being recognized, fear of opening email or electronic communications, and is generally unable to concentrate.

232. Plaintiff has and continues to confer with medical professionals about the symptoms she is suffering as a result of data breaches, and how the data breaches have generally impacted her overall health. Plaintiff's experiences go far beyond allegations of mere worry or inconvenience; they are exactly the sort of injury and

harm to a Data Breach victim that the law contemplates and addresses.

233. Plaintiff has also suffered actual injury in the form of damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breaches.

234. Plaintiff does not recall ever learning that her private medical information and photographs were compromised in a data breach incident, other than the data breaches at issue in this case.

235. Plaintiff has a continuing interest in ensuring that her Personal and Medical Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiffs and Class Members Suffer Damages

236. Defendants negligently, and unlawfully, (i) failed to reasonably secure their patients' information, allowing malicious actors to access, copy, publish and disseminate extremely sensitive patient information; (ii) failed to adequately notify their patients of the breach (but rather misled them); (iii) failed to mitigate the harm by refusing to take reasonable steps to contain the further dissemination of the highly sensitive information; and (iv) failed to prevent a further intrusion into Defendants' computer systems, thus (v) ultimately allowing it to happen all over again. Notwithstanding that Defendants were on notice of the exact risks realized, they failed to secure his patients' data. This is egregious conduct evincing a willful disregard of Plaintiffs' and Class Members' rights and safety.

237. The Data Breaches resulted from Defendants' inadequate cybersecurity and affirmative acts, which exposed Class Plaintiffs' and Class Members' confidential information to unauthorized cybercriminals who exfiltrated it. To date, Defendants have not disclosed the full details of the Data Breaches nor the findings of any investigations.

238. The Data Breaches were directly caused by Defendants' failure to

employ reasonable cybersecurity measures and protocols to protect patients' information. Specifically, Defendants stored confidential data on a network left vulnerable to infiltration, thus permitting the hacking to succeed. Moreover, Defendants stored extremely sensitive patient data – *i.e.*, nude and during-surgery photographs – on inadequately secured portions of their network accessible via the internet. Defendants were aware of the known, prevalent threat of cyberattacks, recognizing that lacking security measures would leave Class Plaintiffs' and Class Members' information in jeopardy.

239. The consequences of Defendants' brazen failure to protect patients' confidential data are severe and enduring. Once stolen, such data can be misused for years. According to the Department of Justice, victims of data breaches are statistically more likely to experience identity fraud.

240. Both federal and state law generally prohibit healthcare providers from disclosing patients' confidential medical information without prior authorization.

241. Beyond statutory obligations, Defendants owed Plaintiffs and Class Members a common law duty to protect their confidential information by exercising reasonable care in obtaining, securing, safeguarding, deleting, and protecting it from unauthorized access, misuse, or disclosure.

242. As a direct result of Defendants' reckless and negligent conduct, unauthorized parties accessed, acquired, and misused Class Plaintiffs' and Class Members' confidential information, invading their privacy, exposing them to an increased risk of identity theft, public disclosure, and fraud.

243. Identity theft has serious consequences. While some victims resolve issues quickly, others spend significant time and money repairing damage to their credit, financial standing, and personal reputation. Some victims may lose job opportunities, be denied loans, or even face wrongful criminal charges due to fraudulent use of their identities.

244. Other potential consequences include fraudulent loans, unauthorized

medical services billed under victims' names, tax fraud, and credit card fraud. In this case, the potential consequences, which were known and foreseeable to Defendants, include public disclosure of patients' private medical information and images.

245. Class Plaintiffs' and Class Members' confidential information has inherent value. Due to the breach, its value has diminished, while Defendants unjustly benefitted from failing to disclose their inadequate security measures.

246. Defendants had ample resources to prevent the breach but deliberately failed to implement adequate security measures, despite their legal obligations to protect patient data. Had Defendants implemented industry-recommended security measures, the breach and subsequent theft of Class Plaintiffs' and Class Members' confidential information could have been prevented.

247. Stolen confidential information can be exploited alone or combined with other publicly available data to commit additional fraud and wrongdoing. Hackers use such data for spear-phishing schemes, impersonating legitimate institutions to deceive victims into revealing even more sensitive information.

248. Additionally, the stolen information includes highly sensitive and humiliating videos and photographs of Class Plaintiffs and Class Members nude, partially clothed, under anesthesia, and undergoing surgery. The release and threatened release of this data has caused and will continue to cause severe emotional distress to Class Plaintiffs and Class Members, compounding the harm.

249. Due to Defendants' wrongful actions and omissions, Plaintiffs and Class Members face ongoing risks, including:

a. The incessant threat of dissemination of private information including PII and PHI, medical diagnosis, extremely sensitive videos and images.

b. Fraudulent use of their confidential information;

c. Financial losses from identity theft;

d. Emotional distress and anxiety;

e. Future costs related to fraud prevention and monitoring.

250. Class Plaintiffs and Class Members have an undeniable interest in ensuring their confidential information remains secure and is not subject to further unauthorized access or misuse.

251. Defendants disregarded Class Plaintiffs' and Class Members' rights by willfully, recklessly, or negligently failing to protect their data systems; failing to disclose their inadequate computer systems and security practices; failing to take reasonable steps to prevent the Data Breaches; failing to monitor and detect the Data Breaches promptly; and failing to provide accurate and timely notice regarding the Data Breaches.

252. Because Defendants did not implement or adhere to reasonable data security protocols, Class Plaintiffs' and Class Members' PII and PHI was obtained by bad actors. Plaintiffs and Class Members have sustained or face a substantial risk of identity theft and fraud, forcing them to invest significant time and money to safeguard against further harm. They remain indefinitely vulnerable to heightened risk of identity theft and fraud.

253. Additionally, this is class is mainly comprised of vulnerable women particularly suspectable to humiliation on the basis of their appearance. Many victims here suffer from a disfiguring conditions and have endured a lifetime of stares, glares, taunts and hurtful comments. Particularly distressing is the fact that nude photos and videos of class members' bodies (including some while under anesthesia) linked with their names, faces, and other identifying information, have been published not only on the dark web, but also on the public internet.

CLASS ACTION ALLEGATIONS

254. Class Plaintiffs bring this action as a class action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and all other similarly situated persons in the following class:

All persons residing in the United States whose personal and medical

information was compromised as a result of the Data Breaches (the "Class"). The Class excludes (a) Defendants and their relatives, employees, agents, attorneys, insurers, and representatives; (b) the Court and its staff; and (c) any persons who give notice that they wish to be excluded from the class pursuant to procedures to be specified by the Court.

255. Class Plaintiffs, including Jane Does A and E, also bring this action on behalf of a subclass comprised of:

All members of the Class who resided in California at the time of either of the Data Breaches (the "California Subclass").

256. Plaintiffs reserve the right to amend the definitions of the Class and California Subclass, and to add additional subclasses.

257. The Court should permit this action to be maintained as a class action pursuant to Federal Rule of Civil Procedure 23, because each of the requirements for class treatment is satisfied.

258. **Numerosity:** The Class is so numerous that the individual joinder of all members is impracticable. Plaintiffs are informed and believe that there are many hundreds if not thousands of total class members, and the class members are geographically dispersed. Plaintiffs are further informed and believe that there are more than 100 members of the California Subclass.

259. **Typicality**. Class Plaintiffs' claims are typical of those of other class members. Each of the Class Plaintiffs had their sensitive Personal and Medical Information accessed and exfiltrated during the cybersecurity attacks described above.

260. **Commonality**. The claims of Class Members raise many common legal and factual issues, which predominate over any individualized issues, including, without limitation, the following:

a. Whether Class Members' Personal and Medical Information stored on Defendants' system constituted protected personal identifying information and/or protected health information under state and federal law;

b. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Class Plaintiffs' and Class Members' Personal and Medical Information

c. Whether and when Defendants actually learned of the First Hack and Second Hack and whether their response was adequate under law;

d. Whether Defendants were required under California and/or federal law to promptly notify affected patients of the data breaches;

e. Whether Defendants did promptly notify patients of the Data Breaches;

f. Whether Defendants owed a duty to the Class to exercise due care in collecting, obtaining, storing and/or safeguarding their Personal and Medical Information;

g. Whether Defendants breached that duty;

h. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the risk of storing Class Plaintiffs' and Class Members' Personal and Medical Information;

i. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Class Plaintiffs' and Class Members' Personal and Medical Information secure and prevent loss or misuse of that information;

j. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breaches to occur;

k. Whether Defendants caused Class Plaintiffs and Class Members damages through their negligent conduct and violation of statute;

l. Whether Defendants violated the California Unfair Competition Law (Business & Professions Code § 17200, et seq.);

m. Whether Defendants violated the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, et seq.); and

n. Whether Class members are entitled to actual damages, credit

monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

261. **Adequacy**: Class Plaintiffs are adequate representatives of the Class. Class Plaintiffs are aware of their fiduciary obligations to Class Members, will fairly and adequately protect those interests, and have no disabling conflicts that would be antagonistic to those of Class Members. Class Plaintiffs have retained competent counsel, experienced in consumer class actions and other complex litigation.

262. **Superiority and Manageability**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein in view of the large number of victims. It will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

263. The nature of this action and the nature of laws available to Class Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged. Absent class proceedings, Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative.

264. Defendants are located and headquartered in California, are licensed in California, all plaintiffs were treated in California, on information and belief, all managerial decisions are made in California, and all the omissions and affirmative

acts complained of herein occurred within California. Thus, application of California law is appropriate.

265. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

266. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

267. Unless a Class-wide injunction is issued, Class Plaintiffs and Class Members remain at risk that Defendants will continue to fail to properly secure their confidential information, resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breaches, and continue to act unlawfully as set forth in this Complaint.

268. Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

FIRST CLAIM

VIOLATION OF THE

CONFIDENTIALITY OF MEDICAL INFORMATION ACT

[Cal. Civ. Code § 56, *et seq.*]

(By Plaintiffs and the Class Against All Defendants)

269. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

270. At all relevant times, Defendants Drs. Schwartz, Total Lipedema Care, and Medva were providers of healthcare within the meaning of California Civil Code § 56.06 and maintained medical information as defined by California Civil Code § 56.05. ModMed is and at all relevant times was deemed provider of healthcare

services pursuant to California Civil Code § 56.06(a) as a "business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care … or for the diagnosis and treatment of the individual."

271. Plaintiffs and Class Members are patients of Defendants, as defined in California Civil Code § 56.05(k).

272. Plaintiffs and Class Members provided their personal medical information to Defendants.

273. At all relevant times, Defendants collected, stored, managed, and transmitted Plaintiffs' and Class Members' personal medical information.

274. Defendants were required by the CMIA to:

a. ensure that medical information regarding patients was not disclosed, disseminated, or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding patients (Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101);

b. refrain from disclosing medical information without first obtaining patient authorization (Cal. Civ. Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104);

c. create, maintain, preserve, and store medical records in a manner that preserved the confidentiality of the information contained therein (Cal. Civ. Code §§ 56.06 and 56.101(a));

d. protect and preserve confidentiality of electronic medical information of Plaintiffs and the Class in their possession (Cal. Civ. Code §§ 56.06 and 56.101(b)(1)(A)); and

e. take appropriate preventive actions to protect confidential information or records against release consistent with Defendants' obligations (Cal. Civ. Code § 56.36(2)(E)).

275. As a result of the Data Breaches, Defendants have misused, disclosed, and/or allowed third parties to access, misuse, disclose, and view Plaintiffs' and Class Members' personal medical information without their written authorization compliant with the provisions of CMIA.

276. The malicious actors who committed the Data Breaches obtained Plaintiffs' and Class Members' personal medical information, viewed it, and now have it available to sell or otherwise disclose for further misuse. They have already disclosed certain of that information both on the dark web and publicly.

277. Defendants' misuse and/or disclosure of medical information regarding Plaintiffs and Class members constitutes a violation of California Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

278. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and Class Members' personal medical information was disclosed without written authorization.

279. By disclosing Plaintiffs' and Class Members' confidential information without their written authorization, Defendants violated California Civil Code § 56, *et seq*., and their legal duty to protect the confidentiality of such information.

280. Defendants also violated Sections 56.06 and 56.101 of the California Civil Code, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

281. Defendants' failure to preserve and negligent mishandling of the Class Plaintiffs and Class Members Personal Medical Information constitutes a violation of California Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

282. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that caused the Data Breaches, Plaintiffs' and Class members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiffs' and Class members' written authorization.

283. Defendants' negligent and reckless failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class members' medical information in a manner that preserved the confidentiality of the information violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). Accordingly, Defendants' systems and protocols did not protect and preserve the integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101.

284. As a direct and proximate result of Defendants' and/or their employees' above-described conduct in violation of the CMIA, Plaintiffs and Class Members were injured and have suffered damages, as described above, from Defendants' illegal disclosure and/or negligent release of their medical information in violation of California Civil Code §§ 56.10 and 56.101.

285. Plaintiffs and Class members are therefore entitled to statutory damages of one thousand dollars ($1,000) for each violation under California Civil Code § 56.36(b)(1); the amount of actual damages, if any, for each violation under California Civil Code § 56.36(b)(2); injunctive relief; and attorneys' fees, expenses, and costs.

SECOND CLAIM

NEGLIGENCE

(By Plaintiffs and the Class Against All Defendants)

286. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

Negligence

287. As a condition of receiving services, Plaintiffs and Class Members were obligated to provide Defendants directly, or through affiliates, with their confidential information.

288. Plaintiffs and Class Members entrusted their Personal and Medical Information to Defendants with the understanding that Defendants would safeguard their information and properly maintain security policies and procedures to prevent data breaches of their data systems.

289. Defendants had full knowledge of the sensitivity of the Personal and Medical Information and the types of harm that Plaintiffs and Class Members could and would suffer if that information were wrongfully disclosed.

290. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, leaked, and/or disclosed to unauthorized individuals. This duty includes, among other things, designing, maintaining, implementing, and testing security protocols to ensure that Personal and Medical Information in their possession was adequately secured and protected, and that employees and vendors tasked with maintaining such information were adequately trained on relevant cybersecurity measures.

291. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Personal and Medical Information of Plaintiffs and Class Members, the critical importance of providing adequate security for that information, the ongoing cyber threats and malicious actions being perpetrated against others in the medical field, and that their training, education, and IT security protocols were insufficient to secure the information of Plaintiffs and Class Members.

292. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' misconduct included, but was not limited to, failing to take reasonably necessary steps to prevent the Data Breaches as set forth herein. Defendants' misconduct also included their decision not to comply with HIPAA and industry standards for the safekeeping and authorized disclosure of patient confidential information of Plaintiffs and Class Members.

293. Plaintiffs and Class Members had no ability to protect their Personal and Medical Information that was in Defendants' possession.

294. Defendants were in a position to protect against the harm suffered by

Plaintiffs and Class Members as a result of the Data Breach.

295. Defendants have at least partially admitted that Plaintiffs' and Class members' confidential information was wrongfully disclosed to unauthorized third persons as a result of the Data Breaches.

296. Defendants have at least partially admitted that Class Plaintiffs' and Class Members' Personal Medical Information was wrongfully disclosed and leaked to unauthorized individuals as a result of the Data Breaches and Defendants' failure to maintain proper security protocol for their Data Systems by way of the Data Breach Notice, and otherwise.

297. Through their actions and omissions, Defendants unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Personal and Medical Information while it was within Defendants' possession or control. Defendants improperly and inadequately maintained Class Plaintiffs' and Class Members' Personal Medical Information in deviation of standard industry rules, regulations, and practices at the time of the Data Breaches.

298. Through their actions and omissions, Defendants unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' confidential information.

299. Through their actions and omissions, Defendants unlawfully breached their duty to adequately disclose to Plaintiffs and Class members the existence and scope of the Data Breaches.

300. Through their actions and omissions, Defendants failed to take reasonable steps to mitigate harm caused by their negligence including attempting to contain the further dissemination of private information.

301. But for Defendants' negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' confidential information would not

have been compromised and/or misused by unauthorized third parties to engage in fraudulent activity and public disclosure that further harmed Plaintiffs and Class Members.

302. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the confidential information and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and the Class.

303. As a result of Defendants' negligence, unauthorized parties acquired Plaintiffs' and Class Members confidential information and used that information to harm Plaintiffs and Class Members as described above.

304. As a further result of Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer damages and injury including, but not limited to:

a. Severe emotional distress due to humiliation, shock, worry and anxiety over the incessant threat of publication, and actual publication, of confidential information including humiliating photos and videos of nude bodies and sensitive medical procedures along with identifying information, as well as identity theft;

b. actual identity theft;

c. an increased risk of identity theft, fraud, and/or misuse of their confidential information;

d. the loss of control over how their confidential information is used;

e. the compromise, publication, and/or theft of their information;

f. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their confidential information, and the value of their time in seeking to mitigate damages;

g. diminished value of the confidential information;

h. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breaches, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from data breaches and identity theft;

i. the continued risk to their confidential information, which remains in Defendants' possession and is subject to further unauthorized disclosures as long as Defendants fail to undertake appropriate and adequate measures to protect confidential information in their continued possession; and

j. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the confidential information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

Negligence Per Se

305. Violations of statutes that establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se*. In addition to the statutes previously set forth, specific statutes governed the handling of Plaintiffs' and Class Members' sensitive information.

306. Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect confidential information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

307. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' confidential Personal and Medical Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Personal and Medical Information they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

308. Defendants' violation of Section 5 of the FTC Act constitutes negligence

per se.

309. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

310. The harm that occurred as a result of the Data Breaches is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

311. Defendants' violation of HIPAA also independently constitutes negligence per se.

312. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and setting forth the conditions under which such information can be used, and to whom it can be disclosed. These privacy laws apply not only to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient, where exposure of such information could present a risk of harm to the patient's finances or reputation.

313. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

314. The harm that occurred as a result of the Data Breaches is the type of harm HIPAA privacy laws were intended to guard against.

315. The Data Breaches resulted from a combination of inadequacies, resulting in Defendants' failure to comply with the safeguards established under HIPAA, including the following:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or

hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incident that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

316. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to, an increased risk of identity theft, fraud, and/or misuse of their confidential information, damages from lost time and effort to mitigate the actual and potential impact of the Data Breaches on their lives, *e.g.*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports. Plaintiffs and Class Members have also suffered severe emotional distress as alleged above.

317. Plaintiffs and Class Members have also suffered damages, which may take months if not years to discover and detect.

318. Defendants' conduct, as alleged herein, was willful, fraudulent, and malicious. Defendants deliberately disregarded the need to safeguard Plaintiffs' and Class Members' confidential information and were willfully indifferent to the risk to Plaintiffs and Class Members of wrongful access to and disclosure of their confidential information. In addition, Defendants misled Plaintiffs and Class Members as to the facts surrounding the Data Breaches, including the nature and scope of the breaches, and the reasons the breaches occurred.

THIRD CLAIM

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §§ 17200, ET SEQ. ("UCL")

(By Plaintiffs and the Class Against All Defendants)

319. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

320. The California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq.* ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and

relevant case law.

321. By reason of Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breaches, and the unauthorized disclosure of Plaintiffs and Class Members' confidential information, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

322. In the course of conducting their business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII/PHI, and by violating the statutory and common law alleged herein, including, inter alia, California's CMIA (Civ. Code §§ 56.10(a), (e); 56.101(a), 56.101(b)(1)(A); 56.36), the California Consumer Privacy Act of 2018 ("CCPA") (Cal. Civ. Code § 1798.150(a)(1)), the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1302d; 45 C.F.R. §§ 164.306(a), (d), (e); 164.308(a); 164.312(a), (d), (e); 164.316(a), (b)), California Civil Code § 1798.81.5, and Article I, Section 1 of the California Constitution (constitutional right to privacy).

323. Defendants also violated the UCL by failing to adequately and timely notify Plaintiffs and Class members pursuant to California Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII/PHI. Had Plaintiffs and Class Members been adequately and timely notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI and identities.

324. Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breaches, and the unauthorized release and disclosure of Plaintiffs' and Class Members' Personal and Medical Information also constitute "unfair" business acts and practices within the meaning of the UCL in that Defendants' conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and the gravity of

Defendants' conduct outweighs any alleged benefits attributable to such conduct. Said acts, omissions and inaction violated strong public policies embodied in the California Constitution, the CMIA, the CCPA, California Civil Code § 1798.81.5, and HIPAA.

325. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the Data Breaches in a timely and accurate manner, contrary to the duties imposed by Cal. Health & Safety Code § 1280.15(b)(2).

326. Plaintiffs and Class members suffered (and continue to suffer) injury in fact, invasion of privacy, and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their confidential information.

327. Plaintiffs and Class members lost money or property by paying for services from Defendants, including a certain level of security for their PII/PHI, but receiving a lower level. Plaintiffs and Class members either paid for services that they would not have obtained had they known of Defendants' lax cybersecurity practices, or paid more for Defendants' products and services than they otherwise would have paid had they known Defendants were not providing the reasonable security represented in Defendants' stated privacy policies and as required by law. Defendants' security practices have economic value in that reasonable security practices reduce the risk of theft of PII/PHI collected, maintained, and stored by Defendants.

328. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class Members' confidential information and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class members.

329. Plaintiffs seek prospective injunctive relief, including improvements to Defendants' data security systems and practices, in order to ensure that such security

is reasonably sufficient to safeguard patients' private information that remains in Defendants' custody.

330. Unless such class-wide injunctive relief is issued, Defendants will continue to engage in the above-described wrongful conduct, more data breaches will occur, Plaintiffs and Class Members will remain at risk, and there is no other adequate remedy at law that would ensure Plaintiffs (and other consumers) can rely on Defendants' representations regarding data security in the future.

331. Furthermore, in the alternative to legal remedies sought herein Plaintiffs and the class further seek restitution of money or property that Defendants have acquired by means of Defendants' unlawful and unfair business practices; disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices; declaratory relief; attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5); and injunctive or other equitable relief.

FOURTH CLAIM

INVASION OF PRIVACY

(By Plaintiffs and the Class Against All Defendants)

332. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

333. California established the right to privacy in Article 1, Section 1 of the California Constitution.

334. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their Personal and Medical Information and were entitled to protection of this information against disclosure to unauthorized third parties.

335. Defendants owed a duty to patients, including Plaintiffs and Class Members, to keep their confidential information confidential.

336. The unauthorized access to and release of confidential information, especially personal health information, photographs, and video, is highly offensive to a reasonable person.

337. The intrusion was into a place or thing, which was private and entitled to be private. Plaintiffs and Class Members disclosed their Personal and Medical Information to Defendants as part of their use of Defendants' medical services, with the intention and reasonable understanding that the confidential information would be kept confidential and protected from unauthorized access and disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

338. The Data Breaches constitute an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

339. Defendants acted with a knowing state of mind when they knowingly failed to adopt and implement adequate cybersecurity practices and protocols to prevent the Data Breach. Defendants knew their data systems were inadequate when they were first hacked in October of 2023, and then hacked again in March of 2024. On information and belief, Defendants knew their systems were not properly encrypted and secured and were defectively designed, and knew that staff and vendors were not properly trained to avoid cyber attacks, and their cybersecurity practices were inadequate which would result in Data Breaches such as the ones that harmed Class Plaintiffs and Class Members.

340. Acting with knowledge, Defendants had notice that their inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

341. As a proximate result of Defendants' acts and omissions, Plaintiffs' and Class Members' confidential information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiffs and Class Members to suffer damages.

342. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to

Plaintiffs and Class Members in that the confidential information maintained by Defendants can be viewed, distributed, and used by unauthorized persons.

343. Plaintiffs and Class members have no adequate remedy at law for the injuries because a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class members.

FIFTH CLAIM

VIOLATION OF CAL. CIV. CODE § 1798.80 ET SEQ.

(By Plaintiffs Jane Doe A and Jane Doe E and the California Subclass Against All Defendants)

344. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

345. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay ...."

346. The California Customer Records Act ("CCRA") further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

347. Any person or business that is required to issue a security breach notification under the CCRA shall be written in plain language and contain the

following information:

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. The date of the breach;

ii. The estimated date of the breach; or

iii. The date range within which the breach occurred.

iv. The notification shall also include the date of the notice. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

348. The Data Breaches described herein constituted a "breach of the security system" of Defendants.

349. As alleged above, Defendants unreasonably delayed informing Plaintiffs and Class Members about the Data Breaches, affecting their Personal and Medical Information, after Defendants knew the Data Breaches had occurred.

350. Defendants failed to disclose to Plaintiffs and members of the California Subclass, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal and Medical Information when Defendants knew or reasonably believed such information had been compromised.

351. Defendants' ongoing business interests gave Defendants incentive to conceal the Data Breaches from the public to ensure continued revenue, which Defendants did for many months.

352. Upon information and belief, no law enforcement agency instructed Defendants that timely notification to Plaintiffs and California Subclass members would impede its investigation.

353. As a result of Defendants' violation of California Civil Code § 1798.82, Plaintiffs and California Subclass members were deprived of prompt notice of the Data Breaches and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and California Subclass members because their stolen information would have had less value to identity thieves.

354. In addition, Defendants' failure to notify appropriate authorities also prevented public disclosure of the Data Breaches through government agencies and the news media. As a result many victims, who were entitled to and otherwise would have received notice that their data had been compromised, were deprived of notice.

355. As a result of Defendants' violation of California Civil Code § 1798.82, Plaintiffs and California Subclass members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breaches itself.

356. Plaintiffs and Class members seek all remedies available under California Civil Code § 1798.84, including, but not limited to, the damages suffered by Plaintiffs and California Subclass members as alleged above and equitable relief.

357. Because Defendants' violations were willful, intentional, and/or reckless, Plaintiffs seek civil penalties not to exceed $3,000 per violation or, in the alternative, $500 per violation pursuant to California Civil Code § 1798.84, as well as attorney's fees and costs.

SIXTH CLAIM

BREACH OF IMPLIED CONTRACT

(By Plaintiffs and the Class Against All Defendants)

358. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

359. Plaintiffs and the Class delivered their Personal and Medical Information to Defendants as part of the process of obtaining treatment and services provided by Defendants.

360. Plaintiffs and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendants an implied covenant of good faith and fair dealing by which Defendants were required to perform their obligations and manage Plaintiffs' and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendants.

361. In providing their Personal and Medical Information, Plaintiffs and Class Members entered into an implied contract with Defendants whereby Defendants, in receiving such data, became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Personal and Medical Information.

362. In delivering their Personal and Medical Information to Defendants, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard that data.

363. Plaintiffs and the Class Members would not have entrusted their Personal and Medical Information to Defendant in the absence of such an implied contract.

364. Defendants accepted possession of Plaintiffs' and Class Members' Personal and Medical Information.

365. Had Defendant disclosed to Plaintiffs and Class Members that Defendants

did not have adequate computer systems and security practices to secure patients' Personal and Medical Information, Plaintiffs and members of the Class would not have provided their Personal and Medical Information to Defendants.

366. Defendants recognized that patients' Personal and Medical Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and Class Members.

367. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

368. Defendants breached their implied contracts with Plaintiffs and Class Members by failing to take reasonable measures to safeguard their data.

369. Defendants breached the implied contract with Plaintiffs and Class Members by failing to promptly notify them of the access to and exfiltration of their Personal and Medical Information.

370. As a direct and proximate result of the breach of the contractual duties, Plaintiffs and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiffs and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of their Personal and Medical Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Personal and Medical Information; (g) the diminution in the value of the services bargained for as Plaintiffs and Class Members were deprived of the data protection and security that Defendants promised when Plaintiffs and the proposed class entrusted Defendants with their Personal and Medical Information; and (h) the continued and substantial risk to Plaintiffs' and Class Members' Personal and Medical Information, which remains in the Defendant's possession with inadequate measures to protect

Plaintiffs' and Class Members' Personal and Medical Information.

SEVENTH CLAIM

UNJUST ENRICHMENT

(By Plaintiffs and the Class Against All Defendants)

371. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

372. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

373. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing Personal and Medical Information to Defendants.

374. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and the Class. Defendants also benefited from the receipt of Plaintiffs' and the Class's Personal and Medical Information, as this was used to facilitate the treatment, services, and goods it sold to Plaintiffs and the Class.

375. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and the Class's Personal and Medical Information because Defendants failed to adequately protect their Personal and Medical Information. Plaintiffs and the proposed Class would not have provided their Personal and Medical Information to Defendants had they known Defendants would not adequately protect their Personal and Medical Information.

376. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

EIGHTH CLAIM

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT,

CAL. CIV. CODE § 1798.150 ET SEQ.

(By Plaintiffs Jane Doe A and Jane Doe E

and the California Subclass Against All Defendants)

377. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

378. Defendants violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Personal and Medical Information of Plaintiffs and the California Subclass. As a direct and proximate result, Plaintiffs', and the California Subclass's nonencrypted and nonredacted Personal and Medical Information was subject to unauthorized access and exfiltration, theft, or disclosure.

379. Defendants are businesses organized for the profit and financial benefit of their owners according to California Civil Code § 1798.140, that collect the personal information of their patients and customers, and whose annual gross revenues exceed the threshold established by California Civil Code § 1798.140(d).

380. Plaintiffs and California Subclass Members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards Personal and Medical Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continues to hold Personal and Medical Information, including Plaintiffs' and California Subclass members' Personal and Medical Information. Plaintiffs and California Subclass members have an interest in ensuring that their Personal and Medical Information is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

381. Pursuant to California Civil Code § 1798.150(b), on August 6, 2025, Plaintiffs e-mailed a CCPA notice letter to counsel for the Schwartz Defendants and counsel for ModMed, detailing the specific provisions of the CCPA that Defendants have violated and continue to violate. Following the filing of this consolidated complaint, MEDVA was also provided a CCPA notice letter.

382. Counsel for Schwartz Defendants responded to the notice on September 9,

2025, but did not offer an adequate cure. Counsel for ModMed did not substantively respond. As such, Plaintiffs seek statutory damages as permitted by the CCPA as against these defendants. Plaintiffs will also seek to amend this complaint to allege statutory damages against MEDVA as permitted by the CCPA to the extent MEDVA does not cure the issues.

383. As described herein, an actual controversy has arisen and now exists as to whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

384. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendants.

PRAYER FOR RELIEF

WHEREFORE, Class Plaintiffs, on behalf of themselves and all members of the Class, pray for relief as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and any subclasses requested herein, appointing the undersigned as Class Counsel, and finding that each of the named Plaintiffs is an appropriate representative of the certified Class;

B. Injunctive relief requiring Defendants to (1) adopt, implement, and maintain reasonable data security systems that maintain personally identifying information to comply with the applicable law and industry standards; (2) engage third-party auditors and internal personnel to determine the scope of the Data Breaches and the patients whose records were compromised; (3) conduct security testing and audits on Defendants' systems on a periodic basis to ensure compliance; (4) promptly correct any problems or issues detected by such audits and testing; (5) conduct periodic training to inform internal personnel how to prevent, identify and contain a breach, and how to appropriately respond; and (6) to provide accurate notice of the nature and scope of the Data Breaches, and the compromised data, to all

affected patients.

C. An award of credit monitoring and identity theft protection services to Plaintiffs and all members of the Class;

D. Actual, compensatory, consequential, incidental, nominal, and statutory damages;

E. Restitution and restitutionary disgorgement;

F. Statutory damages and penalties, trebled, and/or punitive or exemplary damages, to the extent permitted by law, including, but not limited, to the following:

1. Damages not to exceed three thousand dollars ($3,000) per violation, attorney's fees not to exceed one thousand dollars ($1,000) per violation, and the costs of litigation under California Civil Code § 56.35;

2. Statutory damages of one thousand dollars ($1,000) for each violation under California Civil Code § 56.36(b)(1);

3. Actual damages suffered, according to proof, for each violation under California Civil Code § 56.36(b)(2);

4. Damages of $3,000 per violation of Civil Code § 1798.83 or, in the alternative, $500 per violation, pursuant to Civil Code §§ 1798.84(b);

5. Statutory damages of $750 per consumer per incident or actual damages, whichever is greater, under California Civil Code § 1798.150;

G. Punitive damages pursuant to California Civil Code § 3294;

H. Nominal damages according to proof;

I. Attorney's fees pursuant to the common fund doctrine and as provided by law, including, without limitation, under California Civil Code §§ 56.35 and 1798.84, and California Code of Civil Procedure § 1021.5.

J. An award of costs of suit as provided by law;

K. Pre- and post-judgment interest as provided by law;

L. Such other and further relief as the Court may deem just and proper.

///

Dated: October 15, 2025

Respectfully submitted,

BOUCHER LLP

By: /s/ Shehnaz M. Bhujwala
Raymond P. Boucher
Shehnaz M. Bhujwala

Dated: October 15, 2025

Strauss Borrelli PLLC

By: /s/ Raina C. Borelli
Raina C. Borelli
Carly Roman

Interim Co-Lead Class Counsel

DEMAND FOR JURY TRIAL

Class Plaintiffs demand a trial by jury on all matters so triable.

Dated: October 15, 2025

Respectfully submitted,

BOUCHER LLP

By: /s/ Shehnaz M. Bhujwala
Raymond P. Boucher
Shehnaz M. Bhujwala

Dated: October 15, 2025

Strauss Borrelli PLLC

By: /s/ Raina C. Borelli
Raina C. Borelli
Carly Roman

Interim Co-Lead Class Counsel

I attest pursuant to Local Rule 5-4.3.4(a)(2)(i) that all signatories listed, and on whose behalf this filing is submitted, concur in the filing's content and have authorized the filing.

Dated: October 15, 2025

/s/ Shehnaz M. Bhujwala
Shehnaz M. Bhujwala

I, the undersigned, certify that I have filed the foregoing document using the Court's CM/ECF platform. I am informed and believe that filing through the CM/ECF system will result in electronic notice to all parties who have signed up to receive electronic notice, including counsel for all parties who have appeared in the action.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dated: October 15, 2025

/s/ Shehnaz M. Bhujwala
Shehnaz M. Bhujwala